TITANIA

Driving security from PCI DSS 4.0 compliance

Harnessing the power of Nipper Resilience to keep payments data safe - and secure the attack surface, beyond the CDE

Protecting cardholder data

ISAs and QSAs use Nipper on-demand, to assess - with the precision, accuracy and knowhow of a pentester - whether Cardholder Data Environments (CDE) are being adequately protected by correctly configured firewalls, switches and routers, through automated checks that determine the:

- Firewalls' ability to protect the CDE at the perimeter
- Routers' ability to maintain effective network segmentation
- Switches' ability to prevent unauthorized access to the CDE and ensure the integrity of network communications.

Keeping the CDE secure and segmented from other parts of your network is the ultimate mitigating control when it comes to protecting cardholder data. Hardening networks from the inside-out to prevent unauthorized CDE access, instantly reduces the attack surface, and the network infrastructure that needs to comply with PCI DSS.

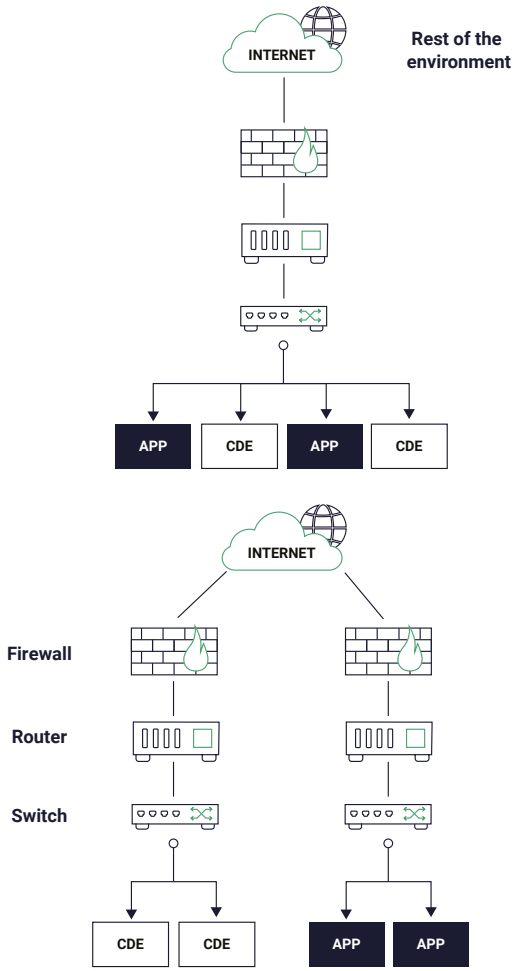
The need for a scalable solution

In Nipper v3.0 and later, relevant device checks have been automatically mapped to PCI DSS 4.0 requirements, and the results are prioritized by compliance risk. Providing evidence-based findings for both passed and failed network checks, as well as any results that require further investigation, enables Nipper to support even greater time savings when needing to demonstrate compliance. For each device tested, findings are listed against applicable PCI DSS requirements, with an explanation of the testing procedure to validate the device's compliance posture.

For non-compliances, Nipper identifies the specific devices affected and provides a risk analysis which determines the ease of exploitation and potential impact to security if exploited. Combined with an ease of fix rating, and command line fix instructions (where possible), Nipper determines the priority for remediation to reduce the mean time to remediate (MTTR) and support compliance posture improvement.

To fully adhere to PCI DSS 4.0, ISAs now also need to regularly assess network infrastructure, and where automation allows, assess all devices, rather than a sample. For what was secure yesterday at the point of audit may no longer be secure today. Using Nipper helps to reduce the assessment of each device by up to 80%, but for compliance teams that frequently need to assess large and/or multiple CDEs, a more scalable solution is required.

Security through segmentation



For what was secure yesterday at the point of audit may no longer be secure today.

Introducing Nipper Resilience

To meet customer's shift in PCI DSS assessment needs, Titania has developed Nipper Resilience, enabling organizations to increase the coverage and cadence of their assessments, and evidence continuous compliance with PCI regulations.

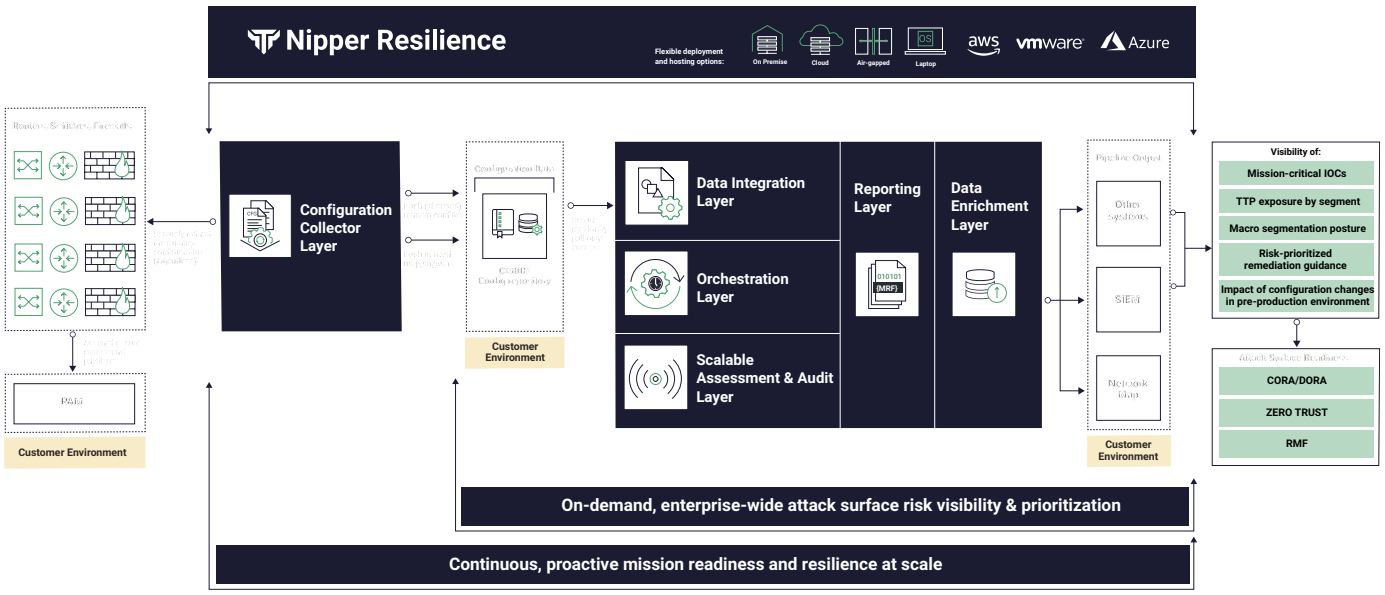
Horizontally scaling Nipper sensors to assess all routers, switches and firewalls in the CDE in one audit, Nipper Resilience aggregates the PCI DSS assessment data, to provide a comprehensive view of compliance risk. Non-compliances are prioritized by risk in a PCI DSS dashboard, with drill-down to the underlying Nipper report findings which recommend how to fix the issues.

Nipper Resilience in action

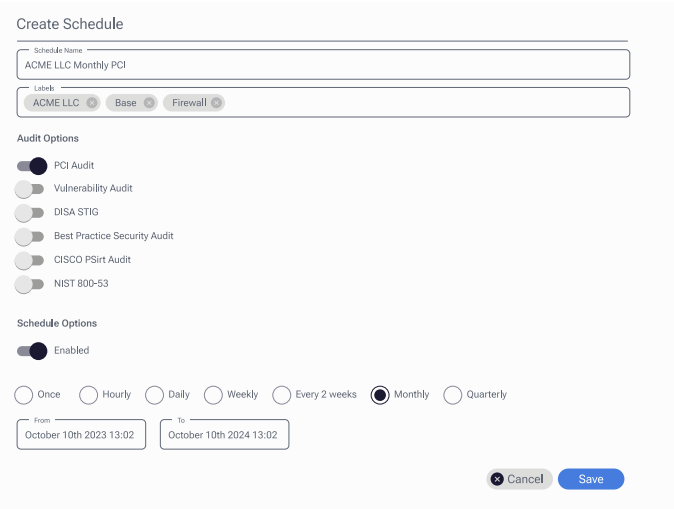
Nipper Resilience passively syncs up to many CMDB and config repositories, pulling down segmentation data to classify device references, without affecting the operational bandwidth of the network. Nipper Resilience allows you to:

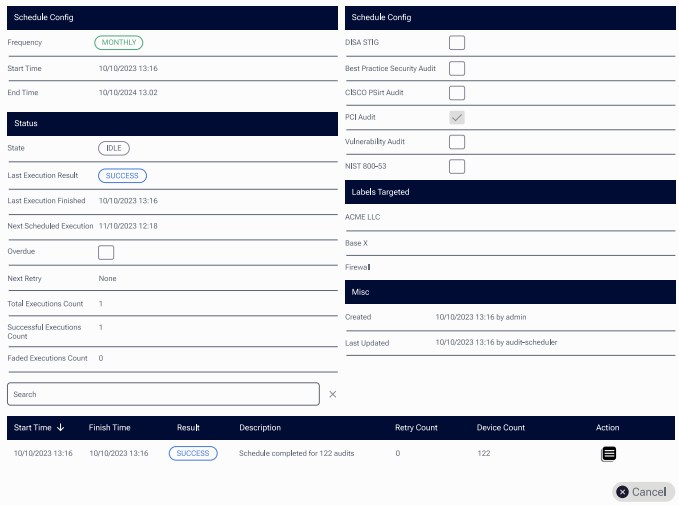
- Sync up to CMDB containing 100,000 devices in as little as 10 mins
- Inherit segment meta data and taxonomy mapping for devices
- Schedule a PCI DSS assessment of your CDE network infrastructure in three easy steps:
  - Identify/target a segment through composition
  - Choose what assessment to perform on matching devices
  - Choose your cadence – how frequently should this assessment be carried out? e.g. Quarterly to support PCI DSS Evidence for Audit or as continuous as daily to drive security from compliance?

How Nipper Resilience aggregates assessment data



Schedule assessments to suit your security and compliance needs





Simple 3-step scheduling

When configurations are synced, PCI DSS assessments of the entire CDE network infrastructure can be scheduled in three simple steps:

1. Firstly, identify the segment you want to assess (e.g ACME Bank LLC -> United Kingdom -> London -> Project X -> CDE)
2. Secondly, choose which assessment to perform on that segment's devices (e.g PCI DSS, NVD/Psirt, Best Practice Security Audit).
3. Finally, set your cadence and control how frequently this assessment should be carried out throughout the year (e.g. quarterly to support PCI DSS evidence for audit, or daily to drive security from compliance)

Nipper Resilience then performs the assessments at the set cadence - on an up to hourly basis as required - and all the evidence is collected and consolidated, which can then be pushed to various platforms including SIEMs (e.g. Elastic or Splunk) and GRCs for visualization and/or further analysis.

Using Nipper Resilience to assess the CDE, enables network owners to:

- Provide accurate compliance posture reports at the point of audit
- Automatically prioritize non-compliances for remediation, based on criticality to CDE security
- Expedite the mean time to remediate non-compliances with ease of fix
- Proactively improve compliance posture by informing remediation workflows
- Easily demonstrate trends in PCI DSS compliance over time

Proactive assessment, effective incident response

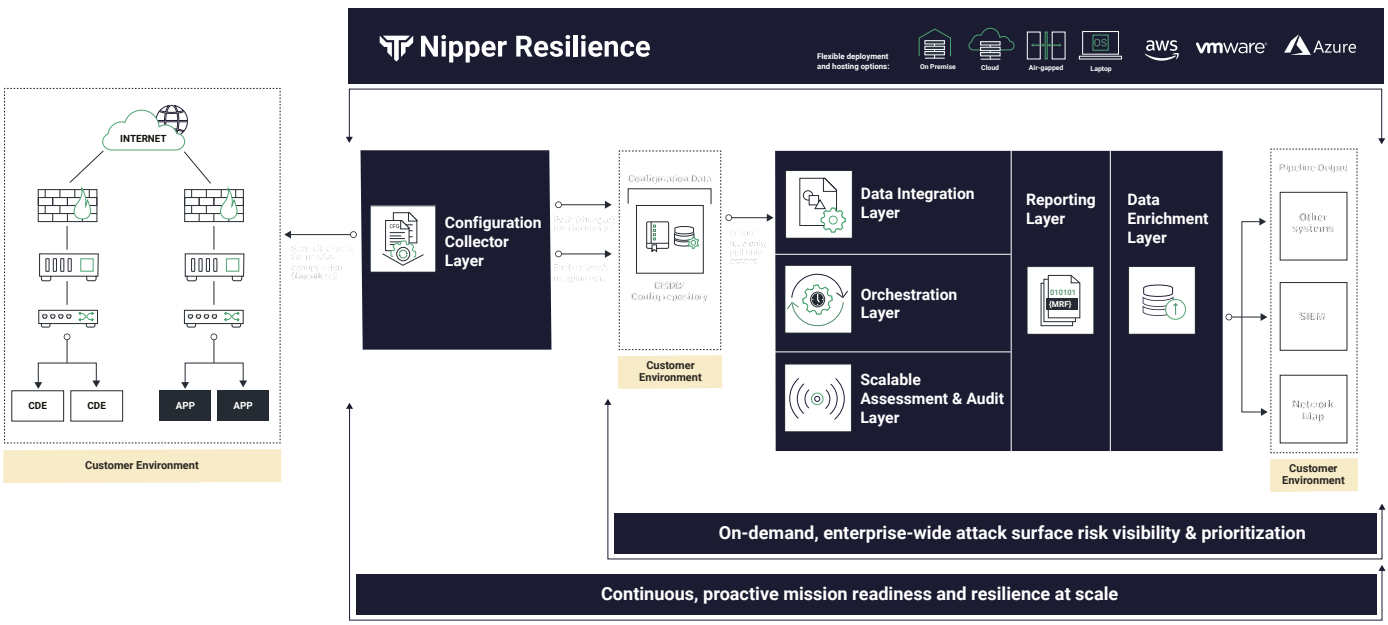
Whilst automating the PCI DSS 4.0 requirements relevant for network devices on the CDE segments on a daily basis is possible with Nipper Resilience, this generates a lot of repetitive data. So Nipper Resilience allows risk owners to apply logic to compliance assessments, and only assess configuration changes to networking devices, between monthly or quarterly audits, to determine whether the CDE has been exposed - either accidentally or nefariously.

Assessing devices after they have been altered can identify indicators of compromise; insight which can inform incident response teams to help shut-down threats in good time. Including threats that come from the inside, such as disgruntled employees or those seeking to expose valuable data for financial gain. For example, if an attacker focuses on non-repudiation by disabling audit logging to conceal their next phase of their attack, they are then free to manipulate firewall rules or create new interfaces to access the CDE segment. And oftentimes a bad actor starts the first phase, then waits to see how effective an organization's incident response is before proceeding. Nipper Resilience's proactive assessment approach stops this kind of attack in its tracks.

Nipper Resilience's proactive assessment capability provides visibility of changes in the CMDB and applies a configurable set of rules, such as "as soon as a device in the CDE segment has changed, perform a PCI DSS 4.0 assessment."

Deployed in this way, Nipper Resilience delivers continuous assessment of the CDE, in a highly practical way.

How Nipper Resilience provides visibility of changes



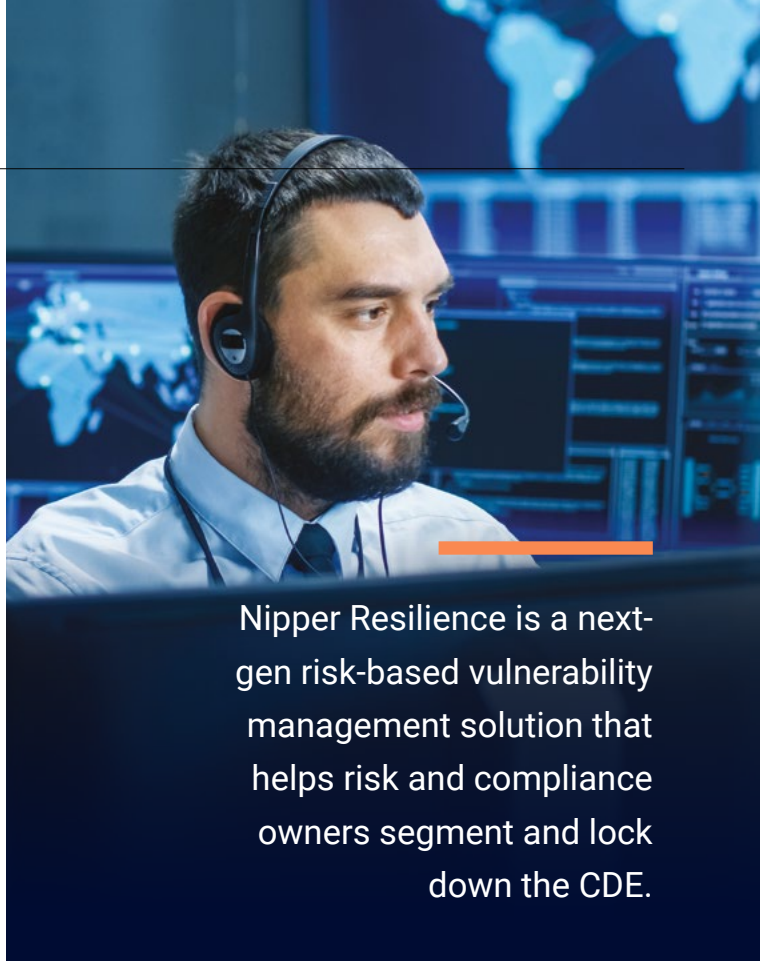
Risk-prioritized remediation that improves PCI DSS compliance posture

Many enterprise organizations are tasked with tens of thousands of networking vulnerabilities at any given time, thanks to out-of-date software. Patching every one simply isn't practicable. And given that only around 8% of all software vulnerabilities have ever been exploited*, it isn't necessary either. Which is why risk-based vulnerability management (RBVM) is increasingly the focus for risk owners.

Nipper Resilience takes RBVM to the next level, enabling network teams to overlay different risk lenses on their PCI DSS compliance posture. For example, overlaying Nipper Resilience's MITRE ATT&CK analysis on the organization's PCI DSS compliance posture highlights which non-compliant misconfigurations and software vulnerabilities are most likely to be targeted by active threats. Informing remediation workflows to address these risks first, would not only demonstrably improve PCI DSS compliance posture, it would drive better security from compliance.

*Source: Gartner, 2023, How To Implement a Risk-Based Vulnerability Management Methodology

For more information, read our MITRE ATT&CK capability statement.



Nipper Resilience is a next-gen risk-based vulnerability management solution that helps risk and compliance owners segment and lock down the CDE.

Security beyond the CDE

Nipper Resilience helps risk and compliance owners to segment and lock down the CDE, but it is also a next-gen vulnerability management solution for securing the attack surface beyond the CDE.

As well as enabling teams to increase the cadence and scale of accurate and detailed network assessments, the range of risk lenses in Nipper Resilience makes it easy to apply to assessment data, providing a transformative, proactive security solution that:

- Reduces the attack surface – minimising the area open to potential threat
- Containerizes threats and prevents the proliferation of attacks, including ransomware
- Makes it easier to implement effective controls and reduce exposure to real world threats
- Neutralizes insider threat – which can be nefarious or accidental leading to external attack
- Supports full control of operational bandwidth.

To discuss your PCI DSS use case, and which solution is the right size for your organization, get in touch to book a demo.

Request a demo to see for yourself how Nipper solutions will be of value to you. **titania.com/try/demo**

Why Titania

At the forefront of proactive network security, Titania's multi-award-winning vulnerability and exposure management solutions are trusted by NOC, SOC, Incident Response and Cyber Protection teams to safeguard critical infrastructure and commercial entities, globally. Whether organizations need real-time visibility and analysis of every network change to get ahead of threats, segmentation violations, and potential network disruptions. Or scheduled network posture and device vulnerability assessments to enhance attack surface security and demonstrate compliance. We have a solution for every stage of the journey to network readiness and resilience.

TITANIA

www.titania.com